ABSTRACT

A system and method for generating and remotely installing a private secure and auditable network is provided. Node identification, link, and application information is input into a template. A generator generates components using the information in the template and the components are remotely installed using an installation server. The components include agent modules which are each installed at predetermined target site and establish communication with the installation server to facilitate the download of other components, including application software and configuration files. Each node can only be installed once and is specific to a predetermined target site. For each link, a unique pair of keys is generated in a form which is not human readable, each key corresponds to a different direction of communication over the link. Data transmitted between nodes is encrypted using public-private key pairs. At least one monitor node manages the security of the network, strobes keys, and may take nodes out of the network in the event of a security violation. In such a case, one or more nodes, or the entire network, may be regenerated and installed anew. Throughout the generation and installation a plurality of verifications, authorizations, and password entries may be required by independent groups to arrive at the network. Preferably, the installation is audited by several groups, and the overall operation may be audited by a second monitor node to detect the presence of an interposed "pirate" node.